CLAIM SUMMARY DOCUMENT:

B1

1. (Previously Amended) A method of controlling the use of a smart card comprising a microprocessor that executes cryptography calculations in the card for effecting authentication sessions at the time of a transaction between the card and a terminal, and at least one control counter, comprising the steps of:

- decrementing or incrementing the control counter by one unit at the start of a transaction comprising at least one authentication session by the card, and

- if the authentication by the card has succeeded, subsequently incrementing or decrementing, respectively, said control counter by said unit.

2. (Previously Amended) A method according to Claim 1 wherein the control counter counts down from or counts up to a blocking value.

3. (Previously Amended) A method according to Claim 2, further including the step of using said control counter by at least one encrypting key contained in the card.

4. (Previously Amended) A method according to Claim 3, wherein the blocking value associated with a counter is a function of the type of transaction in which an associated key is used.

5. (Previously Amended) A method according to Claim 3, wherein the decrementation or incrementation unit of a control counter represents the number of cryptographic calculations with an associated key performed up till then and including the one consisting of said authentication session during said transaction.

B1 cont

6. (Previously Amended) A method according to Claim 3, wherein the control counter associated with a key is decremented or incremented by a new unit before each of the cryptographic calculations using said key up to and including the one relating to said authentication session by the card.

7. (Previously Amended) A method according to Claim 5, wherein the subsequent incrementing or decrementing of the counter by the unit representing the number of cryptographic calculations is effected if the authentication session by the card has succeeded.

8. (Previously Amended) A method according to Claim 6, further including the step of storing the number of decrementations or incrementations by one unit that have been carried out in a pointing counter, to control the subsequent incrementing or decrementing of the control counter via the content of the pointing counter, if the authentication session by the card has succeeded.

9. (Previously Amended) A method according to claim 1, wherein said authentication session by the card is effected at the time of a connection by direct link to a server.

B1 concl'd

10. (Currently Amended) A method according to claim 3 wherein, when the control counter is decremented, or incremented, up to a limit value, it blocks the use of the associated key is blocked.

11. (Previously Amended) A method according to Claim 10, wherein the blocking of the use of the key is irreversible.

12. (Previously Amended) A smart card comprising at least one control counter associated with at least one key and a microprocessor which executes the functions of decrementing or incrementing the control counter by one unit at the start of a transaction comprising at least one authentication session by the card, and subsequently incrementing or decrementing, respectively, said control counter by said unit if the authentication by the card has succeeded.